PERIODICA POLYTECHNICA SER. TRANSP. ENG. VOL. 27, NO. 1–2, PP. 17–28 (1999)

RELIABILITY AND SAFETY RESEARCH OF HOT STANDBY MICROCOMPUTER SIGNALLING SYSTEMS

Christo CHRISTOV* and Nelly STOYTCHEVA**

*Technical University
Sofia, Bulgaria
** Higher School of Transport Engineering
158, Geo Milev Blvd.
1574 Sofia, Bulgaria
Tel./ Fax: (+359 2) 793 075, e-mail: ndsbg@bgnet.bg

Received: Dec. 2, 1999

Abstract

In this paper it has been studied the safety of a widespread class of microcomputer systems for real time control, systems with active redundancy (hot standby), composed of two identical units with three modes of each unit – active, safely failed and dangerously failed states. Markov modelling has been used. Safety is estimated by the dangerous failure function and MTBDF. The aim of the study is to prove that the system's reliability is significantly greater than that of the separate unit while safety does not change sufficiently, which makes the system applicable as a signalling one.

Keywords: reliability, safety, microcomputer signalling systems, hot standby.

1. Introduction

The subject of this investigation is the fault tolerance hot standby microcomputer signalling system. The scheme of such system is shown in *Fig. 1.*

Both units **B** (**basic**) and **R** (**reserve**) consist of information-processing devices (microcomputers, controllers or hard logic's electronic circuits) with built-in self-control instruments **C**, which control their failures. If a failure occurs in any unit, an incorrect signal could appear on its outputs which could have unregulated and even dangerous consequences. Therefore after the failure has been discovered, the self-control instruments **C** act upon a switch **Sw**, which commutes the unit's outputs.

In due time (for a time shorter than the interval t_{DIN} of the **PR** information uncertainty allowed by the process) **PR** cannot accept the applied control signals. This is a time parameter, which characterizes the inertia of the controlled important technological process (**ITP**).

Normally, both units accept simultaneously the initial information **I** from the operator and the control information from **PR** and they are in an equal information state. If a failure is discovered in the unit **B**, **Sw1** switches the control of **ITP** to unit **R**, which underrates it. If the failure is in unit **R**, **Sw2** switches the process off, protecting it from an incorrect and possibly dangerous control.

The so defined **subject** of investigation is *a fault tolerant hot standby system.*

Such systems have been discussed in the literature: HENLEY et al. (1981), KANTZ et al. (1995), GUPTA et al. (1993A), GUPTA et al. (1993B), LIEYU et al. (1992), KRIS et al. (1993), CAO et al. (1989), ZHOU et al (1991). Standby techniques are used to improve system reliability. Here we prove that the system's reliability compared to the separate unit's reliability is significantly greater while safety does not change sufficiently which makes these systems applicable as signalling ones. Such systems are used to **ITP**, which ruin of parameters may lead to a danger for people's life and health or loss of huge material, cultural or natural values.

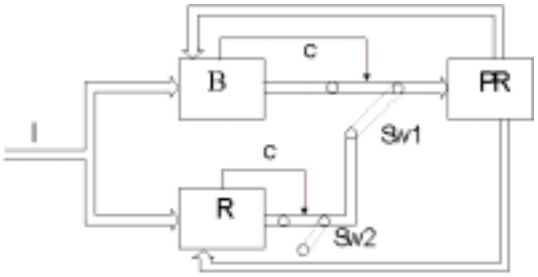

Fig. 1. Scheme of Hot Standby Microcomputer Signalling System

As a method for solving the tasks, pointed above, the theory of Markov's random processes is used: CHRISTOV (1990), CHRISTOV and STOYTCHEVA (1992), SAPOJNIKOV et al. (1995), CHRISTOV and STOYTCHEVA (1995), LAPRIE and MEDHAFFER-KANOUN (1982), QUIRRK (1988), HENLEY and KUMAMOTO (1981), AVIZIENIS et al. (1991), DALE and FOSTER (1987).

2. Description of the Model

The **aspect** in which the hot standby microcomputer system is investigated is the reliability and safety of the system.

Reliability will be measured by two characteristics (CHRISTOV (1990), SAPOJNIKOV et al. (1995), LAPRIE and MEDHAFFER-KANOUN (1982), HENLEY and KUMAMOTO (1981), AVIZIENIS et al. (1991)):

- *Function of Availability* $\mathbf{A}(t)$. It can be proven that for the values of the λ and the μ, that are of practical interest (see Section 4), the availability function $\mathbf{A}(t)$ quickly reaches a constant limited probability, known as the availability coefficient $K_A = \lim_{t\to\infty} \mathbf{A}(t)$ after which the availability is not changed.
- *Mathematical Expectation of Time between Consequent Failures* (the mean time between failures) **MTBF**, which is the reciprocal value of the failure frequency **H**. It shows the failures' number per unit time. It is well known, for

example, from KOCHS (1984), that $\mathbf{H} = K\lambda$. It is known from reliability theory, but in KOCHS (1984) it has common means, available for homogeneous Markov's random processes.

Safety in this paper is investigated in the aspect of the system behaviour after failure, e.g. CHRISTOV (1990), CHRISTOV and STOYTCHEVA (1992), LAPRIE and MEDHAFFER-KANOUN (1982). This technogene safety is regarded as a single feature of reliability. While reliability is determined by any failure of activity, safety is a result only of the dangerous failures. Dangerous is the failure, which has not been discovered from the system by adopted means of control for time t_{DIN}.

The units **B** and **R** as well as the system as a whole can have three states (*Fig. 2*):

1. – **active** (**A**), when correct controlling signals are formed towards the process.
2. – **dangerously failed** (**D**), when the failure remains undiscovered for a time greater than the information uncertainty time allowed by the process. In this case the incorrect controlling signals can have unpredictable, including dangerous consequences.
3. – **safely failed** (**S**), when incorrect output signal is formed, but within the information uncertainty time t_{DIN} allowed by the process, the failure is discovered and the switch **Sw** turns the incorrect signals off.

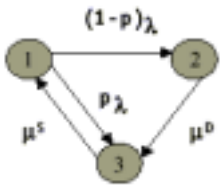

Fig. 2. States of the units **B** and **R**

The transitions between the states are determined by the intensities λ, μ_D and μ_S, as well as by the probability **p** for the failure to be discovered in due time.

Safety in the aspect studied is estimated by the following characteristics:

- *Function of the system failure on the dangerous side* $\mathbf{D}(t)$, which measures the change of the probability the system to be found in dangerously failed state during mission time t. For this parameter is also true what has been said above about availability. In long enough time it reaches a constant value, known as the dangerous coefficient $\mathbf{K}_D$.
- *mean time between the successive dangerous failures* **MTBDF**. This is the time between two successive appearances of a dangerously failed state. It is found as a reciprocal value of the dangerous failure frequency $\mathbf{H}_D$:

$$H_D = K_A(1-p)\lambda. \tag{1.a}$$

MTBF (the reliability parameter) for *Fig. 2* is:

$$\mathbf{MTBF} = \frac{1}{K_S\mu_S}. \tag{1.b}$$

Criterion of a dangerous state D is the presence of a failure, undiscovered for some time after its appearance, as a result of which the **ITP** is reached and accepts incorrect control signals.

Criterion of a safe state S is the presence of a failure, discovered within time t_{DIN} and a transition towards system's recovery.

3. Notation

The following assumptions have been made:

1. The failure and restoration flows of both units are Poisson's.
2. The intensities of the transitions between states $S \to D$ $(3 \to 2)$ and $D \to A$ $(2 \to 1)$ are negligibly small and are not regarded.
3. The commutation mechanism is perfect e.g. failure and error free.

λ	–	failure rate
μ	–	restoration rate
p	–	probability, the unit's failure to be recognised and discovered during the allowed by **PR**
t_{DIN}	–	time of information uncertainty
μ_D	–	restoration rate of the unit's operative state following a safely failed state
μ_S	–	restoration rate of the unit's danger state following a safely failed state
$\mathbf{A}(t)$	–	function of availability
$\mathbf{D}(t)$	–	probability of the system failure on the dangerous side during mission time
$\mathbf{S}(t)$	–	safety probability of the system during stays of the system
$\mathbf{K}_{AV}$	–	availability factor
$\mathbf{K}_N$	–	unavailability factor

$\mathbf{K}_D$ – dangerous coefficient (the probability of the system failure on the dangerous side when time is infinite)
$\mathbf{K}_S$ – safety coefficient (the safety probability of the system when time is infinite.)
H – failure frequency
$\mathbf{H}_D$ – dangerous failure frequency
$\mathbf{B}_A$; $\mathbf{R}_A$ – the basic **B** (the reserve **R**) unit is active
$\mathbf{B}_N$; $\mathbf{R}_N$ – the basic **B** (the reserve **R**) unit is inactive
$\mathbf{B}_i$ $\mathbf{R}_j$ – the basic **B** (the reserve **R**) units' states determining the total state of the system
$i, j \subset A$ – normally operating state
S – state failed on safe side
D – state failed on dangerous side.

Partial state of the system is a vector of reliable safe states of the system's separate units, in which each unit has one own state.

$\mathbf{Pr}_i$ – probability of a partial state
$\mathbf{K}_i$ – limit probabilities of the states
MTBF – Mean Time Between Failure
MTBDF – Mean Time Between Dangerous Failure

4. Model of the Separate Unit's Reliability and Safety

The reliable safe state of each information-processing unit can be described by the diagram in *Fig. 2*, where the states have the meaning given above (Section 2).

At the assumption 1 made above, that the failure and restoration flows are Poisson's which is valid for a broad class of systems, the unit's reliability and safety characteristics can be found through solving the Kolmogorov differential equation system, written for the diagram in *Fig. 2*:

$$\begin{aligned} \frac{\mathrm{d}A(t)}{\mathrm{d}t} &= -[(1-p)\lambda + p\lambda]A(t) + \mu_S S(t), \\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} &= (1-p)\lambda A(t) - \mu_D D(t), \\ \frac{\mathrm{d}S(t)}{\mathrm{d}t} &= p\lambda A(t) + \mu_D D(t) - \mu_S S(t). \end{aligned} \tag{2}$$

Taking a Laplace transform of *Eq.* (2) and solving them gives:

$$\begin{aligned} A(t) &= \frac{\mu_S \mu_D}{r_1 r_2} + \frac{(r_1+\mu_S)(r_1+\mu_D)e^{r_1^t}}{r_1(r_1-r_2)} - \frac{(r_2+\mu_S)(r_2+\mu_D)e^{r_2^t}}{r_2(r_1-r_2)}, \\ D(t) &= \left[\frac{\mu_S}{r_1 r_2} + \frac{(r_1+\mu_S)e^{r_1^t}}{r_1(r_1-r_2)} - \frac{(r_2+\mu_S)e^{r_2^t}}{r_2(r_1-r_2)}\right]\lambda(1-p)s, \end{aligned} \tag{3}$$

$$S(t) = \left[\frac{\mu_D}{r_1 r_2} + \frac{(r_1 \cdot p + \mu_D)e^{r_1^t}}{r_1(r_1 - r_2)} - \frac{(r_2 \cdot p + \mu_D)e^{r_2^t}}{r_2(r_1 - r_2)}\right]\lambda,$$

where:

$$r_{1,2} = \frac{1}{2}\Big[-(\mu_S + \mu_D + \lambda) \pm \sqrt{(\mu_S + \mu_D + \lambda)^2 - 4\{[\mu_S(1-p) + \mu_D]\lambda + \mu_S\mu_D\}}\Big].$$

For the limit state probabilities (time equals infinity) the following expressions come out of (3):

$$\begin{aligned} K_W &= \frac{\mu_D\mu_S}{\mu_D\mu_S + \lambda[\mu_D + \mu_S(1-p)]}, \\ K_D &= \frac{\mu_S\lambda(1-p)}{\mu_D\mu_S + \lambda[\mu_D + \mu_S(1-p)]}, \\ K_S &= \frac{\mu_D\lambda}{\mu_D\mu_S + \lambda[\mu_D + \mu_S(1-p)]}. \end{aligned} \tag{4}$$

Let us accept some probable values of the parameters participating in these formulas:

$$\lambda = 1.10^{-3}\ [1/\text{h}]; \quad \mu_D = 2\ [1/\text{h}]; \quad \mu_S = 0.5\ [1/\text{h}];\ p = 0.99.$$

Substituting in (4) we obtain $K_A = 0.997999$, $K_D = 4.9\ E\ 10^{-6}$ and $K_S = 0.0019959$.

5. Model of the System's Reliability and Safety

5.1. A Diagram of the System's Partial States

First a diagram of the system's partial states is built (*Fig. 3*). The global states of the system are three: active, dangerously failed and safety failed.

Second on the base of the system work and the safety criterion (Section 2) the following connections of the partial states to the global ones are defined:

1. In states 1, 4 and 7 **B** unit is active and regardless of unit **R** state, the system is in an availability state.
2. In state 2 **B** unit is failed on the safe side and in the process is accordingly included **R** unit, which is active. The system is in an availability state.
3. In states 3, 6, 9 **B** unit is failed on the dangerous side and no transition has been realised to **R** unit. The system works dangerously since the failure has not been discovered in **B** unit.
4. In state 5 the units are safely failed and the system is accordingly failed on the safe side.

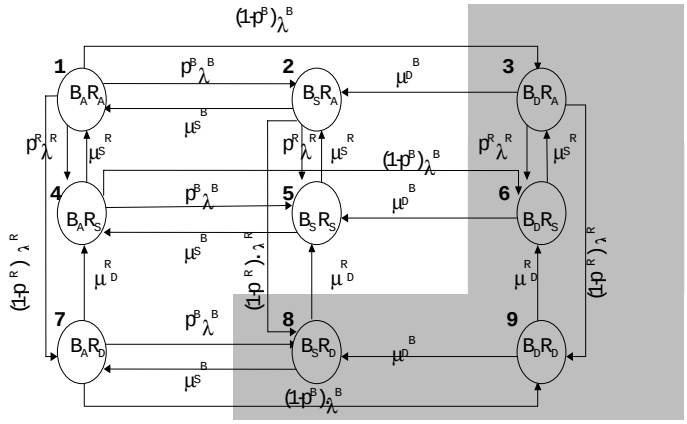

Fig. 3. Markov's diagram of the Hot Standby System

5. In state 8 **B** unit is safely failed and **R** unit is dangerously failed. The system is in a dangerous state as the switching to unit **R** leads to incorrect output signals.

The probability of each system's partial state is obtained as a multiplication of the probabilities of the unit's states, which combination it is of.

$$
\begin{aligned}
&Pr_1 = A(t)^B A(t)^R, \quad Pr_2 = S(t)^B A(t)^R, \quad Pr_3 = D(t)^B A(t)^R,\\
&Pr_4 = A(t)^B S(t)^R, \quad Pr_5 = S(t)^B S(t)^R, \quad Pr_6 = D(t)^B S(t)^R,\\
&Pr_7 = A(t)^B D(t)^R, \quad Pr_8 = S(t)^B D(t)^R, \quad Pr_9 = D(t)^B S(t)^R,
\end{aligned}
\tag{5}
$$

where $\mathbf{A}(t)$, $\mathbf{S}(t)$ and $\mathbf{D}(t)$ are taken from (3).

The limit probabilities of the states on the graph in *Fig. 3* are:

$$
\begin{aligned}
&K_1 = K_{AV}^B K_{AV}^R, \quad K_2 = K_{AV}^R K_S^B, \quad K_3 = K_{AV}^R K_D^B,\\
&K_4 = K_S^R K_{AV}^B, \quad K_5 = K_S^B K_S^R, \quad K_6 = K_D^B K_S^R,\\
&K_7 = K_{AV}^B K_D^R, \quad K_8 = K_S^B K_D^R, \quad K_9 = K_D^B K_D^R,
\end{aligned}
\tag{6}
$$

where K_{AV}^B, K_S^B, K_D^B, K_{AV}^R, K_S^R and K_D^R are determined from (4).

The equivalence of the basic and the reserve unit simplifies the investigation without limiting the generality. Further we are warning at this condition with the simplified formulas.

5.2. Reliability

5.2.1. System Availability

To obtain the availability of the system, the probabilities of active partial states have to be summarised taking into account the units' identity:

$$A_{\text{sys}}(t) = Pr_1 + Pr_2 + Pr_4 + Pr_7 = A(t)[A(t) + 2S(t) + D(t)]. \qquad (7)$$

Taking into account that $A(t) + S(t) + D(t) = 1$ and transferring to limit probabilities, which in the worst case limit the readiness, we obtain:

$$K_{AV\ \text{SYS}} = K_{AV}(1 + K_S). \qquad (8)$$

5.2.2. The Mean Time Between Failure $MTBF_{\text{SYS}}$

The mean time between failure of the system MTBF_{SYS} is defined as the inverse value of the failure frequency of the system incoming the active state:

$$\mathbf{MTBF}_{\text{SYS}} = \frac{1}{H_{\text{SYS}}}. \qquad (9)$$

Following the transitions in the graph in *Fig. 3*, we find from theory of KOCHS (1984):

$$\mathbf{MTBF}_{\text{SYS}} = \frac{1}{K_3\mu_D + 2K_5\mu_S + K_8\mu_S} = \frac{1}{K_{AV}K_D\mu_D + 2K_S^2\mu_S + K_SK_D\mu_S}. \qquad (10)$$

5.3. Safety

5.3.1. Probability of a Dangerous Failure

To obtain the function of the system's dangerous failure, the probabilities of dangerous partial states have to be summarised taking into account the units' identity:

$$D_{\text{SYS}}(t) = Pr_3 + Pr_6 + Pr_8 + Pr_9 = D(t)[A(t) + 2S(t) + D(t)]. \qquad (11)$$

Accounting that $A(t) + S(t) + D(t) = 1$ and transferring to limit state probabilities, which in the worst case limit the danger, we obtain:

$$K_{D\ \text{SYS}} = K_D(1 + K_S). \qquad (12)$$

From the obtained formulas we can draw the conclusion that due to the hot reserve (standby) in the system both the readiness and the dangerous work increase.

5.3.2. MTBDF

Mean Time Between the Dangerous Failures of the system is defined as the reciprocal value of the frequency of falling into dangerous state $H_{D\,\mathrm{SYS}}$.

$$\mathbf{MTBDF}_{\mathrm{SYS}} = \frac{1}{H_{D\,\mathrm{SYS}}}. \tag{13}$$

Following the transitions on the graph in *Fig. 3*:

$$\begin{aligned} H_{D\,\mathrm{SYS}} &= K_A(K_A + K_S + K_D)(1-p)\lambda + K_A K_D p\lambda + K_A K_S(1-p)\lambda \\ &= K_A\lambda[(1-p)(1+K_S) + K_D p]. \end{aligned} \tag{14}$$

We can see that for $p = 1$, when $K_D = 0$ (see *Eq.* (4)) , the frequency of falling into a dangerous state is zero and the time $\mathbf{MTBDF}_{\mathrm{SYS}}$ tends to infinity.

6. Comparative Analysis of the Reliability and Safety Indexes of the System and its Comprising Units

In order to estimate qualitatively the effect of introducing the dynamic redundancy as a second unit in the hot standby regime, we will compare the time parameters, which determine the **MTBF** of the system and the time between its successive dangerous failures with the analogous indexes for its comprising units.

6.1. Comparison by Reliability

To figure out how the system's lifetime is improved in comparison to the unit's lifetime, the following ratio is built:

$$\xi = \frac{\mathbf{MTBF}_{\mathrm{SYS}}}{\mathbf{MTBF}} = \frac{K_s\mu_S}{2K_{AV}K_D\mu_D + 2K_S^2\mu_S + K_S K_D\mu_D}, \tag{15}$$

where $\mathbf{MTBF}_{\mathrm{SYS}}$ is known from (10) and MTBF is known from *Eq.* (1.b). Substituting from (4) in (15) and transforming it, we obtain:

$$\xi = \frac{\mu_D\mu_S + \lambda\mu_D + \lambda(1-p)\mu_S}{\mu_D\mu_S(1-p) + 2\lambda\mu_D + \lambda(1-p)\mu_S}. \tag{16}$$

It is clear that the prolonging of the expected lifetime of the system depends on all primary parameters of reliability and safety of the comprising units. For example the dependence $\xi(p)$ on the probability p to discover the failure on time is linear and represents a part of a hyperbola, whose lowest point is at $p = 0$:

$$\xi = \frac{\mu_D\mu_S + \lambda\mu_D + \lambda\mu_S}{\mu_D\mu_S + 2\lambda\mu_D + \mu_S\lambda} \tag{17}$$

and the highest at $p = 1$:

$$\xi = \frac{\mu_S + \lambda}{2\lambda}. \tag{18}$$

For the accepted above values of the terms included in the formulas (Section 4) it can be established that for $p = 1$ $\xi = 250$. On the other side if $p = 0.99$ $\xi = 72$, i.e. the reliability, measured by the expected lifetime of the system, is orders of magnitude better than that of the separate unit.

6.2. Comparison by Safety

To understand the influence of the structure on the system's safety, we can form the ratio:

$$\eta = \frac{\mathbf{MTBDF}_{\mathrm{SYS}}}{\mathbf{MTBDF}}, \tag{19}$$

which reveals the change of the system's safety as compared to the unit's safety, measured by this parameter. Using *Eqs.* (1.a) and (13) and substituting in (19) we obtain:

$$\eta = \frac{1-p}{(1-p)(1+K_S)+K_D p} = \frac{\mu_D\mu_S + \lambda(1-p)\mu_S + \lambda\mu_D}{\mu_D\mu_S + \lambda\mu_S + 2\lambda\mu_D}. \tag{20}$$

It is obvious that the expected time between the dangerous failures of the system depends on all primary reliability and safety parameters of the units, that is comprised of. For example, the dependence $\xi(p)$ on the probability p to discover the failure in due time, is linear and decreases from

$$\eta = \frac{\mu_D\mu_S + \lambda\mu_S\lambda\mu_D}{\mu_D\mu_S + \lambda\mu_S + 2\lambda\mu_D} \qquad \text{at } p = 0 \tag{21}$$

to

$$\eta = \frac{\mu_D(\mu_S + \lambda)}{\mu_D\mu_S + \lambda\mu_S + 2\lambda\mu_D} \qquad \text{at } p = 1. \tag{22}$$

As it was shown above in this case both times between the dangerous failures – of the unit and of the system – tend to infinity and this ratio starts to lose its realistic meaning.

It was seen, that in the worst case at the practically interesting values of the terms, participating in the dependence, the ratio η is lowest but very close to 1. For the adopted above values of the parameters included in the formulas it can be established that for $p = 1$ $\eta = 0.997511$ and for $p = 0.99$ $\eta = 0.9979641$, i.e. the mathematical expectation of the time between the dangerous failures of the system drops only by about 0.2% in comparison to what may be expected for the separate unit.

7. Conclusions

1. The introduction of the second unit as a hot standby (reserve) expresses exclusively in the increasing of the system's reliability. The mathematical expectation of the system lifetime is much greater than that of the separate unit and depends on its reliable safe parameters p, λ and μ. The effect of the reserve is as stronger as higher is the discovery of the failure p.
2. The increasing of the discovery of the failures p leads to the decreasing of the dangerous work probability both of the unit and of the system. The reserving worsens the system's safety in comparison to that of the unit but its influence is extremely low and practically it can be considered that the system preserves the same safety as the unit with reliability improved by orders of magnitude.

References

[1] AVIZIENIS, A. – KOPETZ, H. – LAPRI, L. C. (1991): Dependability Basic Concept and Terminology, Springer Verlag, Wien, New York, 1991.
[2] CAO, J. – WU, Y. (1989): Reliability Analysis of a Two-Unit Cold Standby System With Replaceable Repair Facility, *Microelectronics and Reliability*, Vol. 29, No. 2, pp. 145–150.
[3] CHRISTOV, CH. – STOYTCHEVA, N. (1992): Algorithms for Analytical Modelling of Signaling System Safety, *Scientific Conference of Higher School of Transport Engineering*, Sofia, 1992, pp. 122–132 (In Bulgarian).
[4] CHRISTOV, CH. – STOYTCHEVA, N. (1995): Railway Real-time Control Systems Modelling of Dynamic Redundant Systems Reliability, *Second International Scientific Conference 'Modern Supply Systems and Drives for Electric Traction'*, Conference Proceedings, Poland, Warsaw, October, 1995, pp. 42–47.
[5] CHRISTOV, CH. (1990): Theory of the Signalling System, Technika, Sofia, 1990 (In Bulgarian).
[6] DALE, C. – FOSTER, S. (1987): The Development of Techniques for Safety and Reliability Assessment: Past, Present and Future, Achieving Safety and Dependability With Computing System, Wiley, 1987.
[7] GUPTA, P. P. – SHARMA, M. K. (1993): Reliability and MTTF Evaluation of a Two Duplex-Unit Standby System With Two Types of Repair, *Microelectronics and Reliability*, Vol. 33, No. 3, 1993, pp. 291–295.
[8] GUPTA, R. – CHAUDHARY, A. (1993): A Multi-component Standby System Subject to Inspection and Truncated Normal Failure Time Distribution, *Microelectronics and Reliability*, Vol. 33, No. 2, pp. 127–131, 1993.
[9] HENLEY, E. – KUMAMOTO, H. (1981): Reliability Engineering and Risk Assessment, 1981.
[10] JIEYU SHE – PECHT, M. G. (1992): Reliability of a *k*-out of-*n* Worm-Standby System, *IEEE Transactions on Reliability*, Vol. 42, No. 1, 1992.
[11] KANTZ, H. – KOZA, CH. (1995): The ELEKTRA Railway Signalling-System: Field Experience with an Actively Replicated System with Diversity, *The Twenty-Fifth International Symposium on Fault-Tolerant Computing*, Pasadena, California, June 27–30, 1995, pp. 453–458.
[12] KOCHS, H. D. (1984): Zuverlässigkeit elektronischer Anlagen, Berlin, Heidelberg, New-York, Tokio, 1984.
[13] KRIS, B. – GANDJO, S. (1993): Analysis of a Repairable Two-unit Parallel Redundant System with Failure and Repair Times Arbitrarily Distributed, *Microelectronics and Reliability*, Vol. 33, No. 3, pp. 307–312, 1993.
[14] LAPRIE, J. – MEDHAFFER-KANOUN, K. (1982): Dependability Modelling of Safety Systems, *Microelectronics and Reliability*, Vol. N12, 1982, pp. 997–1024.

[15] QUIRK, W. J. (1988): Principles for Design for Safety, *Safety of Computer Control System, SAFECOMP'88, Proceedings of the IFAC Symposium*, FRG,1988, pp. 101–106.
[16] SAPOJNIKOV, VL. V. – SAPOJNIKOV, V. V. – CHRISTOV, CH. – GAVZOV, D. V. (1995): Methods for Design of Microelectronic Railway Signaling and Telemechanics Systems, Transport, Moscow, 1995 (In Russian).
[17] ZHOU, ZH. – YUAN, C. (1991): Reliability Measures for Fail-Safe Computer-Based Systems, *Microelectronics and Reliability*, Vol. 31, No. 2/3, pp. 401–406, 1991.